

日 本 国 特 許 庁
JAPAN PATENT OFFICE

#2
3/19/02
JP

Jc979 U.S. PTO

10/052282



別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application:

2001年 6月11日

出 願 番 号

Application Number:

特願2001-174981

出 願 人

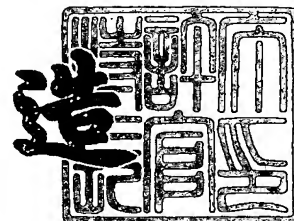
Applicant(s):

株式会社日立製作所

2001年11月26日

特 許 庁 長 官
Commissioner,
Japan Patent Office

及 川 耕 造



出証番号 出証特2001-3102400

【書類名】 特許願

【整理番号】 K01001231A

【あて先】 特許庁長官

【国際特許分類】 G06F 17/60

【発明者】

【住所又は居所】 神奈川県川崎市麻生区王禅寺 1 0 9 9 番地 株式会社日立製作所 システム開発研究所内

【氏名】 吉川 達也

【発明者】

【住所又は居所】 神奈川県川崎市麻生区王禅寺 1 0 9 9 番地 株式会社日立製作所 システム開発研究所内

【氏名】 鮫嶋 茂稔

【発明者】

【住所又は居所】 神奈川県川崎市麻生区王禅寺 1 0 9 9 番地 株式会社日立製作所 システム開発研究所内

【氏名】 河野 克己

【発明者】

【住所又は居所】 東京都千代田区神田駿河台四丁目 6 番地 株式会社日立製作所 情報制御システム事業部内

【氏名】 中野 利彦

【発明者】

【住所又は居所】 茨城県ひたちなか市市毛 1 0 7 0 番地 株式会社日立製作所 ビルシステムグループ内

【氏名】 小林 延久

【特許出願人】

【識別番号】 000005108

【氏名又は名称】 株式会社日立製作所

【代理人】

【識別番号】 100075096

【弁理士】

【氏名又は名称】 作田 康夫

【手数料の表示】

【予納台帳番号】 013088

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 分散システムにおけるサービス提供方法

【特許請求の範囲】

【請求項 1】

所定のサービスを提供するための情報処理を実行するサービスデバイスと、前記サービスデバイスに対して前記サービスの要求を示す要求情報を送信する要求デバイスとからなる分散システムにおいて、

前記サービスデバイスが、前記要求デバイスから送信される前記要求情報を受信するステップと、

前記サービスデバイスが、当該サービスデバイスの所定範囲内の状況を示す周辺情報を収集するステップと、

前記サービスデバイスが、前記周辺情報に基づいて、前記要求情報で要求されるサービスを提供可能な場合は、提供可能な前記サービスを提供するための情報処理を実行するステップとを有することを特徴とする分散システムにおけるサービス提供方法。

【請求項 2】

請求項 1 に記載の分散システムにおけるサービス提供方法において、

前記周辺情報には、前記サービスデバイスおよび前記要求デバイスの少なくとも一方から所定範囲内に、予め定められた周辺デバイスが存在するか否か示す情報が含まれ、

前記情報処理を実行するステップでは、前記周辺デバイスが前記所定範囲内に存在する場合に、前記情報処理を実行することを特徴とする分散システムにおけるサービス提供方法。

【請求項 3】

請求項 2 に記載の分散システムにおけるサービス提供方法において、

前記周辺デバイスは、前記サービスを受ける権限を有することを示す識別情報を記憶することを特徴とする分散システムにおけるサービス提供方法。

【請求項 4】

請求項 1 乃至 3 のいずれかに記載の分散システムにおけるサービス提供方法に

において、

前記サービスデバイスは、サービス毎に当該サービスを提供する場合の条件を対応付けた拡張アクセスコントロールリストを記憶する記憶装置と接続し、

前記情報処理を実行するステップは、収集された前記周辺情報が前記条件に対応する場合に、前記情報処理を実行することを特徴とする分散システムにおけるサービス提供システム。

【請求項5】

請求項4に記載の分散システムにおけるサービス提供方法において、

前記拡張アクセスコントロールリストには、前記条件が、前記周辺情報に応じて、前記サービスを受けることが可能な利用者もしくは要求デバイスを変更されて格納されることを特徴とする分散システムにおけるサービス提供方法。

【請求項6】

請求項1乃至5のいずれかに記載の分散システムにおけるサービス提供方法において、

前記サービスを提供するための情報処理には、前記要求デバイスから前記サービスデバイスへのアクセスが含まれることを特徴とする分散システムにおけるサービス提供方法。

【請求項7】

所定のサービスを提供するための情報処理を実行するサービス提供装置において、

前記サービスの要求を示す要求情報を送信する要求デバイスから前記要求情報を受信する受信装置と、

前記受信装置と接続され、記憶装置に格納されたプログラムに従って、当該サービス提供装置の所定範囲内の状況を示す周辺情報を収集し、前記周辺情報に基づいて、前記要求情報で要求されるサービスを提供可能な場合は、提供可能な前記サービスを提供するための情報処理を実行する処理装置とを有することを特徴とするサービス提供装置。

【請求項8】

請求項7に記載のサービス提供装置において、

前記周辺情報には、前記サービスデバイスおよび前記要求デバイスの少なくとも一方から所定範囲内に、予め定められた周辺デバイスが存在するか否か示す情報が含まれ、

前記処理装置は、前記周辺デバイスが前記所定範囲内に存在する場合に、前記情報処理を実行することを特徴とするサービス提供装置。

【請求項 9】

請求項 8 に記載のサービス提供装置において、

前記周辺デバイスは、前記サービスを受ける権限を有することを示す識別情報を記憶することを特徴とするサービス提供装置。

【請求項 10】

請求項 7 乃至 9 のいずれかに記載のサービス提供装置において、

サービス毎に当該サービスを提供する場合の条件を対応付けた拡張アクセスコントロールリストを記憶する記憶装置をさらに有し、

前記処理装置は、収集された前記周辺情報が前記条件に対応する場合に、前記情報処理を実行することを特徴とするサービス提供装置。

【請求項 11】

請求項 10 に記載のサービス提供装置において、

前記処理装置は、前記記憶装置に、前記条件を、前記周辺情報に応じて、前記サービスを受けることが可能な利用者もしくは要求デバイスを変更して格納することを特徴とするサービス提供装置。

【請求項 12】

請求項 7 乃至 11 のいずれかに記載のサービス提供装置において、

前記サービスを提供するための情報処理には、前記要求デバイスから前記サービスデバイスへのアクセスが含まれることを特徴とするサービス提供装置。

【請求項 13】

所定の領域への人間の入場を管理する入場管理システムにおいて、

前記領域への入場を物理的に制限する制限装置と、

前記制限装置と接続する手段と、前記制限手段を開放する開放要求を、要求装置から受信する手段と、所定範囲内に、前記領域への入場が許可される個人また

は組織を識別する情報が格納された周辺装置が存在するかを検知する手段と、前記周辺装置が存在する場合に、前記制限装置に対し、前記領域への入場を許容する制御を実行する手段とを有する制御装置と

を備えたことを特徴とする入場管理システム。

【請求項 1 4】

請求項 1 3 に記載の入場管理システムにおいて、

前記制限装置は、錠を備えたドアであり、

前記制御装置は、前記周辺装置が存在する場合に、前記錠を開錠するよう制御することを特徴とする入場管理システム。

【請求項 1 5】

請求項 1 3 または 1 4 のいずれかに記載の入場管理システムにおいて、

前記検知する手段は、前記所定範囲に所定の信号を無線で発信し、発信された無線に対する応答に応じて、検知することを特徴とする入場管理システム。

【発明の詳細な説明】

【 0 0 0 1】

【発明の属する技術分野】

本発明は、所定の機能を実行するデバイスの制御に関するものである。この中でも、アクセスコントロールリスト(ACL)などの情報を用いて各デバイスをアクセス制御する方式のセキュリティ分野を対象としている。また、さらに、入退出管理や盗難防止、物品管理等において適用可能な技術に関する。

【 0 0 0 2】

【従来の技術】

従来、デバイスが複数存在する分散システムにおけるアクセス制御方法として、例えば特開 2 0 0 0 - 1 1 2 8 9 1 号公報に記載されている方法がある。これによると、システム内の各デバイスに分散アクセスコントロールリスト(ACL)を個別に持たせることによって、ユーザ属性に応じたアクセス制御を行っていた。また、設定対象の計算機にその都度ログインすることなしに当該設定を可能とすることで、設定の手間を軽減し設定ミスを防止していた。

【 0 0 0 3】

【発明が解決しようとする課題】

上記従来技術においては、様々なユーザが訪問するオフィスビル等において、制限区域内に重要物が存在する場合には入室を禁止し、そうでない場合は許可するような場面を想定した時、従来の画一的なアクセス制御では運用/管理者のアクセスレベルの設定変更作業やユーザの設定変更要求からの時間的な遅れという点で限界があった。

【0004】

本発明は、分散システムにおいてユーザ及びサービスデバイスの状況に応じて、より柔軟なアクセス制御を実現することを目的とする。

【0005】

【課題を解決するための手段】

上記目的を達成するために、本発明は、デバイスの周辺情報に応じて、アクセス制御を含むサービス提供のための情報処理を行うものである。周辺情報は、デバイスの所定範囲内の状況を示す情報であり、サービス提供の条件となるものである。周辺情報には、所定デバイスから所定の範囲内にある他のデバイスの状態を示す情報が含まれる。他のデバイスの状態には、他のデバイス（予め定められた）が存在するか否か、他のデバイスの運転状況が含まれる。また、周辺情報には、デバイスから所定範囲内に、サービスを受ける者が存在するか、またその者がサービスを受ける権利を有する者かを示す情報が含まれる。

【0006】

本発明には、所定のサービスを提供するサービスデバイスから所定範囲内に、サービスを要求する要求デバイスと、サービスデバイスもしくは要求デバイスから所定範囲内に、要求デバイスにサービスを受ける権限を与える周辺デバイスが存在するか否かに従って、サービスデバイスが所定のサービスを提供するかどうかを制御する。サービスデバイスが入出場を制御するドア等で、要求デバイスが携帯電話で、周辺デバイスが電子的に個人または組織を識別する情報が格納されたIDカードである場合の例を説明する。この例では、所定の部屋に入場するためにドアの鍵を開ける指示を、携帯電話からドアに送信する。ドアの鍵の開閉を制御する制御装置は、指示を受付けるとドアもしくは携帯電話から所定範囲内に

、当該部屋への入場が許可される個人を識別するIDカードが存在すれば、携帯電話からの要求に対応してドアの鍵を開ける。IDカードの存在は、制御装置から電波を発して行ってもよい。

【0007】

また、本発明には、サービスデバイスへアクセス可能なデバイス（サービスを受けることが可能な利用者）を、周辺情報に応じて、に替えることも含まれる。

【0008】

【発明の実施の形態】

以下、本発明の実施例を図1により説明する。

図1は、本発明におけるアクセス制御システムの適用形態例を示す。主な構成要素としては、サービスデバイス（電子錠）0114に対してサービスを要求するユーザ0110、ユーザインタフェースを提供する携帯端末0111、携帯端末0111の周辺に存在する同伴者0112が所有するユーザ周辺デバイス（IDカード、携帯端末等）0113、ユーザの要求するサービスを提供するサービスデバイス（電子錠）0114、サービスデバイス（電子錠）0114の周辺に存在する不審者0115が所有する機器周辺デバイス（未登録IDカード、携帯端末等）0116等からなる。

【0009】

図2は、本発明におけるアクセス制御システムの構成図である。主な構成要素としてユーザ0210、携帯端末0211、サービスデバイス0220、ユーザ周辺デバイス0218、機器周辺デバイス0228から構成される。このシステムは環境中に複数デバイスが分散して存在し、各サービスデバイス0220のハードディスク領域には拡張アクセスコントロールリスト(Extended Access Control List:EACL)0223が格納され、共通通信プロトコルを用いた無線通信モジュール(所定の通信技術を用いることができる)を有する。ユーザ0210は携帯端末0211(携帯電話/PDA等)を介して必要なサービスを要求し、サービスデバイス0220よりサービスを受信する。ユーザ0210は携帯端末0211を用いて、個人認証情報(ユーザID:676001027、グループID:105u)/サービス情報(要求サービスID:応接室開錠)をサービスデバイスに対して送信する。

【0010】

ただし、個人認証情報は携帯端末0211に記憶、サービス情報はネットワーク経由で入手したサービス一覧より選択する。携帯端末0211上の周辺デバイス検知処理0216は、携帯端末0211上の通信処理0217に対して周辺デバイス検索信号を送信する。通信管理処理0217は、周辺デバイスに対してデバイス情報配信要求信号を同報配信する。無線通信内に存在するユーザ周辺デバイス0218はデバイス情報配信要求信号を受信すると、通信処理0219によって周辺デバイス固有のグローバルユニークなID（周辺デバイスID：F0032A8）や周辺デバイスの状態（稼動中、スリープ等）を携帯端末上の通信処理0217に対して送信する。周辺デバイス情報を受信した通信処理0217は、周辺デバイス検知処理0216に情報を配信する。周辺デバイス情報を受信した周辺デバイス検出処理0216は、ユーザ周辺デバイス情報DB0214内のテーブルに周辺デバイス情報を書き込む。

【0011】

さらに、周辺デバイス検出処理0216はユーザ0210から最初に送信された個人認証情報/要求サービス情報に周辺デバイス情報を併せて、サービスデバイス0220に送信する。周辺デバイス検出処理0216は常時起動しており、一定周期でユーザ周辺デバイス0218の検出を行う。ユーザ情報/ユーザ周辺情報を受信したサービスデバイス0220上のアクセス制御処理0222は、サービスデバイス0220の周辺デバイス0213の情報収集を自身の機器周辺デバイス検出処理0225に対して要求する。要求を受信した機器周辺デバイス検出処理0225は、前記の携帯端末0211上のユーザ周辺デバイス検出処理0216と同様の処理によって、機器周辺デバイス0228の情報を獲得する。併せて、周辺デバイス情報DB0226内のテーブルに獲得した周辺デバイス情報を書き込む。機器周辺デバイス検出処理0225は、獲得した周辺デバイス情報をアクセス制御処理0222に配信する。

【0012】

周辺デバイス情報を受信したアクセス制御処理0222は、サービスデバイス0220上に記憶されたEACL0223を参照する。その際、携帯端末0211か

ら受信したユーザ情報/ユーザ周辺情報及び前記のサービスデバイス周辺情報を利用する。アクセス制御処理 0 2 2 2 は、受信した情報（ユーザID、グループID、要求サービスID、ユーザ周辺デバイス情報、機器周辺デバイス情報）とEACL 0 2 2 3を照合することによって、アクセスレベルを決定する。但し、ユーザ 0 2 1 0やユーザ周辺デバイス 0 2 1 8の履歴情報 0 2 3 0を参照してアクセスレベルを決定する場合もある。その際は、EACL 0 2 2 3を参照して決定されたアクセスレベルと比較を行い、ある政策（例えば、アクセスレベルの低い方を採用する等）に従ってアクセスレベルを決定する。アクセス制御処理 0 2 2 2は決定されたアクセスレベルのモードでサービスデバイス 0 2 1 2を制御し、ユーザ 0 2 1 0にサービスを提供する。その際の情報/サービスの流れについては、図 3 から図 9で詳述する。

【 0 0 1 3 】

尚、サービスデバイス 0 2 2 0は、ユーザ 0 2 1 0からのサービス要求時のみならず、上記ユーザ個人情報及びユーザ周辺情報を任意のタイミングで送信要求することが可能であることを付記する。

【 0 0 1 4 】

図 3 は、本発明におけるシステム全体の処理を示すフローチャートである。S T 0 3 1 0において、ユーザ 0 2 1 0は携帯端末 0 2 1 1を介してサービスデバイス 0 2 2 0に対してサービスを要求する。その際、ユーザ 0 2 1 0は携帯端末 0 2 1 1を介して明示的にユーザID、グループID及び要求サービスIDを入力するか、携帯端末 0 2 1 1に予め記憶された各項目を選択しサービスデバイス 0 2 2 0に対してメッセージを送信する。S T 0 3 1 1においては、ユーザ情報のメッセージ送信要求を受けた携帯端末 0 2 1 1はユーザ周辺デバイス 0 2 1 8の検索を開始する。携帯端末 0 2 1 1は、ユーザ周辺デバイス 0 2 1 8よりデバイス情報を受信する。

【 0 0 1 5 】

また、他に周辺デバイスが存在しないかどうかチェックを行い、ユーザ周辺デバイス 0 2 1 8が存在すれば処理を繰り返す。ユーザ周辺デバイス 0 2 1 8が存在しなければ、S T 0 3 1 2に進む。S T 0 3 1 2においては、ユーザ 0 2 1 0

から入力あるいは携帯端末0211上に記憶されたユーザID、グループID、要求サービスIDと、ST0311で獲得したユーザ周辺デバイス情報を併せて、サービスデバイス0220に送信する。

【0016】

ST0313においては、携帯端末0211からサービス要求メッセージを受信すると、機器周辺デバイス0228の探索を開始する。サービスデバイス0220は、機器周辺デバイス0228よりデバイス情報を受信する。また、他に周辺デバイスが存在しないかどうかチェックを行い、機器周辺デバイス0228が存在すれば処理を繰り返す。機器周辺デバイス0228が存在しなければ、ST0314に進む。ST0314においては、携帯端末0211より受信した情報とST0313で獲得した機器周辺デバイス情報を利用してEACLの参照を行い、アクセスレベルを決定する。ST0315においては、ST0314で決定したアクセスレベルに基づいてユーザ0210に対してサービスを提供する。

【0017】

図27は、本発明における履歴情報データベースを用いた場合のシステム全体の処理を示すフローチャートである。ST2710乃至ST2714においては、ST0310乃至ST0314と同一の処理を行う。ST2715は、履歴情報DB0230を参照してアクセスレベルを決定する。決定したアクセスレベルとST2714で決定されたアクセスレベルをある政策（例えば、アクセスレベルの低い方を選択する等）に従ってアクセスレベルを決定する。ST2716においては、ST2715で決定したアクセスレベルに基づいてユーザ0210に対してサービスを提供する。

【0018】

図4は、本発明における携帯端末上の周辺デバイス検出処理を示すフローチャートである。ST0410において、ユーザ0210からI/O0212、アプリケーション0213を介してユーザ情報及びサービス要求を受信する。ST0411においては、通信処理0217に対して周辺デバイス検索要求を送信する。具体的には、各デバイスに対して同報メッセージを送信する要求を出す。ST0412においては、ユーザ周辺デバイス0218から通信処理0217へ送信

された周辺デバイス情報を受信する。ST0413においては、機器構成管理処理0215にユーザ周辺デバイス0218の情報取得要求を送信する。ST0414においては、ユーザ情報及び機器構成管理処理0215から受信した情報をサービスデバイス0220に送信する。

【0019】

図5は、本発明における携帯端末上の機器構成管理処理を示すフローチャートである（非常駐処理）。ST0510において、周辺デバイス検出処理0216からユーザ周辺デバイス情報データベース0214への参照要求を受信する。ST0511においては、ユーザ周辺デバイス情報を元にユーザ周辺デバイス情報データベース0214を参照する。ST0512においては、ST0511で得られた参照結果を周辺デバイス検出処理0216に送信する。

【0020】

図6は、本発明における携帯端末上の機器構成管理処理を示すフローチャートである（常駐処理）。ST0610において、通信処理0217からユーザ周辺デバイス情報を受信する。ST0611において、ユーザ周辺機器情報を元にユーザ周辺デバイス情報データベース0214を参照する。ST0612においては、周辺デバイス検出処理0216にユーザ周辺デバイス0218の状態変更を通知する。次に、ST0610に戻る。

【0021】

図7は、本発明におけるサービスデバイス上の周辺デバイス検出処理を示すフローチャートである。ST0710において、携帯端末0211からサービス要求を受信する。ST0711においては、通信処理0227に対して周辺デバイス検索要求を送信する。具体的には、各デバイスに対して同報メッセージを送信する要求を出す。ST0712においては、機器周辺デバイス0228から通信処理0227へ送信された周辺デバイス情報を受信する。ST0713においては、機器構成管理処理0225に機器周辺デバイス0228の情報取得要求を送信する。ST0714においては、ユーザ情報及び機器構成管理処理0225から受信した情報をアクセス制御処理0222に送信する。

【0022】

図 8 は、本発明におけるサービスデバイス上の機器構成管理処理を示すフローチャートである（非常駐処理）。ST0810において、周辺デバイス検出処理0224から機器周辺デバイス情報データベース0226への参照要求を受信する。ST0811においては、機器周辺デバイス情報を元に機器周辺デバイス情報データベース0226を参照する。ST0812においては、ST0811で得られた参照結果を周辺デバイス検出処理0224に送信する。

【0023】

図 9 は、本発明におけるサービスデバイス上の機器構成管理処理を示すフローチャートである（常駐処理）。ST0910において、通信処理0227から機器周辺デバイス情報を受信する。ST0911において、機器周辺機器情報を元に機器周辺デバイス情報データベース0226を参照する。ST0912においては、アクセス制御処理0222に機器周辺デバイス0228の状態変更を通知する。次に、ST0910に戻る。

【0024】

図 1 0 は、本発明においてユーザが携帯端末を介してサービスを要求する際に送信するメッセージを示した図である。上記メッセージは、通信ヘッダ1010及びデータ1014からなり、その主な構成要素としては、ユーザの個人認証に用いられるユーザID1011、ユーザが属するグループID1012、ユーザがサービスデバイスに対して要求する要求サービス1013等からなる。また、データ1014の主な構成要素としては、ユーザ周辺デバイスに関する周辺機器構成1015、要求サービス1016等からなる。

【0025】

図 1 1 は、本発明におけるユーザから送信の情報示す図である。主な構成要素としては、ユーザからデータが送信された時間を表すデータ送信日時1110、ユーザ個人を特定するユーザID1111、ユーザが属するグループID1112、ユーザ0210がサービスデバイス0220に対して要求する要求サービスID1113等からなる。

【0026】

図 1 2 は、本発明におけるユーザ周辺デバイス情報示す図である。主な構成

要素としては、周辺を検索してデータが得られた時間を表すデータ受信日時 1 2 1 0、ユーザ周辺に存在するユーザ周辺デバイス情報 1 2 1 1 等（ID、状態値等）からなる。但し、ユーザ周辺デバイス情報 1 2 1 1 は、ユーザ周辺デバイス 0 2 1 8 が存在した場合のみ有効である。

【 0 0 2 7 】

図 1 3 は、本発明における周辺デバイス情報を利用した EACL を示す図である。主な構成要素として、ユーザが本 EACL を有するサービスデバイスに対して許可されるアクセスレベル 1 3 1 0、ユーザの属するグループ ID 1 3 1 1、ユーザ周辺に存在する機器のユーザ周辺デバイス情報（ID、状態値等） 1 3 1 2、サービスデバイス周辺に存在する機器周辺デバイス情報（ID、状態値等） 1 3 1 3 からなる。但し、ユーザ周辺情報 1 3 1 2 及び機器周辺デバイス情報 1 3 1 3 は、ユーザ周辺デバイス 0 2 1 8 及び機器周辺デバイス 0 2 2 8 が存在した場合のみ有効である。

【 0 0 2 8 】

図 2 3 は、本発明におけるサービス要求／提供時の時間（帯）によってアクセスレベルが変化する EACL を示す図である。主な構成要素として、受信情報 2 3 1 0、時間（帯） 2 3 1 1、アクセスレベル 2 3 1 2 等から構成される。受信情報 2 3 1 0 は、上記ユーザから受信したグループ ID 1 3 1 1、ユーザ周辺デバイス情報（ID、状態値等） 1 3 1 2、上記サービスデバイス周辺に存在する機器周辺デバイス情報（ID、状態値等） 1 3 1 3 からなる。時間（帯）は、サービス要求あるいはサービス提供時のある時刻あるいはある時間帯を示す。アクセスレベル 3 1 2 は、上記アクセスレベル 1 3 1 0 と同値である。同一の情報を受信した場合でも、サービス要求／提供時刻によって異なったアクセスレベルを提供するものである。

【 0 0 2 9 】

図 1 4 は、本発明におけるアクセスレベルと実行許可処理との関係を示す図である。主な構成要素として、上記アクセス制御処理において決定されたアクセスレベル 1 4 1 0、サービスデバイスで実行され得る実行処理 1 4 1 1、各アクセスレベルにおける実行処理を行うか行わないかを示したアクセス権限 1 4 1 2 等

からなる。

【0030】

図15は、本発明における周辺デバイスの判定基準を示す図である。携帯端末0211やサービスデバイス0212のように周辺デバイス検出処理0214を備えたデバイスi1514を中心とした半径 d_L 1511の円を想定する。ここで、 d_L はデバイス固有の近傍距離閾値である。このとき、その円周を近傍境界線1510として、デバイスi1514と周辺デバイスj1513、非周辺デバイスk1515間の距離を赤外線近接センサ等を用いて測定する。デバイスi1514と周辺デバイスj、非周辺デバイスkとの距離をそれぞれ d_{ij} 1512、 d_{ik} 1512とする。このとき、不等式1516を用いて対象とするデバイスが、デバイスi1514の周辺デバイスj1513であるか、あるいは非周辺デバイスk1515であるかを判定する。

【0031】

図16は、本発明における周辺閾値（近傍距離閾値）を既定方法を示す図である。主な構成要素としては、ユーザ1610、ユーザ周辺デバイス1611、サービスデバイス1612、周辺閾値情報1613、ユーザ情報1614、周辺閾値1615等からなる。ユーザ1610は、携帯端末0211を通じてユーザ情報1614（ユーザID、グループID、要求サービスID等）をサービスデバイス1612に送信する。上記ユーザ情報1614を受信したサービスデバイス1612は、周辺閾値情報DBの参照を行い周辺閾値1615を決定する。

【0032】

その際、利用する情報は、上記ユーザ情報1614及びサービスデバイス1612情報である。決定された周辺閾値1615は、ユーザの所有する携帯端末1610に送信される。携帯端末1610は、受信した周辺閾値1615内を検索範囲1616としてユーザ周辺デバイス1611の探索を行う。但し、ユーザ周辺デバイス1611が同時にサービスデバイス1612の周辺デバイスと認識される場合は、ある政策（例えば、アクセスレベルが下がる方の周辺デバイスと認識する等）に従って処理を行う。

【0033】

図 1 7 は、本発明におけるサービスによる異なる周辺距離の例を示す概略図である。主な構成要素としては、サービス 1 7 1 0、周辺距離 1 7 1 1 等からなる。サービスデバイス 0 2 2 0 の提供するサービスに応じて、ユーザ 0 2 1 0 が探索すべき周辺距離 1 7 1 1（周辺円領域の半径）を規定する。例えば、「ドアの開錠」サービスに対する周辺距離は、「1 0 m」、「ドアの施錠」サービスに対する周辺距離は、「0 m」等である。

【 0 0 3 4 】

図 1 8 は、本発明におけるアクセス制御方法を適用した実施例 1 を示す概略図である。主な構成要素として、部長 1 8 1 0、課長 1 8 1 1、制限区域（金庫）1 8 1 2、不審者 1 8 1 3 等から構成される。課長 1 8 1 1 は、携帯端末 0 2 1 1 として PDA を所有している。また、部長 1 8 1 0 はユーザ周辺デバイス 0 2 1 8 として、自身の情報を登録した ID カードを所有している。また、この適用例のサービスデバイス 0 2 2 0 としては、金庫の電子錠 1 8 1 2 を想定している。また、機器周辺デバイス 0 2 2 8 としては、不審者 1 8 1 3 が所持する未登録品（ID カード等）を考える。そこで、本発明における周辺デバイス情報を用いたアクセス制御システムの適用例における概略は以下に示す通りである。『課長 1 8 1 1 一人では開錠禁止の金庫 1 8 1 2 であるが、部長 1 8 1 0 同伴の場合は開錠が許可される。ただし、金庫 1 8 1 2 付近に不審者 1 8 1 3 が検知された場合開錠されない。』さらに詳述すると、以下のようである。

【 0 0 3 5 】

1. 課長 1 8 1 1 は PDA を用いて、個人認証情報（ユーザ ID : usr_676001027、グループ ID : grp_105）/サービス情報（要求サービス ID : 金庫開錠）1 8 1 4 を送信する。ただし、個人認証情報は PDA に記憶、サービス情報は、ネットワーク経由で入手可能なサービス一覧を用いて、ユーザ 0 2 1 0 が携帯端末 0 2 1 1 から選択する。但し、個人認証情報の PDA の記憶に際しては、メモリ及び SIM/WIM カードを用いた記憶方法等を想定している。

2. 送信データに PDA の周辺デバイス情報である ID カード情報（周辺デバイス情報 : [info_udev] : {id.udev_001, stat.udev_001, ...}）を加えて電子錠 1 8 1 2 に送信する。尚、部長 1 8 1 0 が偶然、課長 1 8 1 1 のそばを通りかかっ

た場合を回避するために、部長 1 8 1 0 は明示的にリーダーに ID カードをかざす。

3. ユーザ周辺デバイス情報（ユーザ ID、状態値等）は共通化された通信プロトコル（BT 等）を利用して、PDA が獲得する。

4. PDA からメッセージ（ユーザ ID、グループ ID、要求サービス ID、ユーザ周辺デバイス情報）1 8 1 4 を受信した電子錠 1 8 1 2 は、機器周辺デバイスである未登録品情報（機器周辺デバイス情報：[info_ddev]：{id.ddev_001, stat.ddev_001, ...}）を獲得する。尚、不審者 1 8 1 3 の特定方法については、不審者 1 8 1 3 の所有する通信機器（ID カード等も含む）への要求に対して、通信そのものは確立されているにも関わらず、応答がない（機器情報を送信しない等）などの場合に対象物を不審者 1 8 1 3 とみなす方法等も含む。

【0036】

5. データ（ユーザ ID、グループ ID、要求サービス ID、ユーザ周辺デバイス情報、機器周辺デバイス情報）と電子錠上の EACL とで照合を行い、アクセスレベルを決定する。

6. 決定されたアクセスレベルのモードで電子錠 1 8 1 2 を制御する。

7. 課長 1 8 1 1 にサービス（金庫を開錠しないというサービス）を提供する。

8. 尚、補足として、金庫内に重要物品がある場合セキュリティシステムが作動し、そうでない場合は複数（例えば、登録された全て）のユーザからの入室許可を認める等の実施例も含むことを付記する。

【0037】

図 1 9 は、本発明におけるアクセス制御方法を適用した実施例 2 を示す概略図である。主な構成要素として、客 1 9 1 0、店員 1 9 1 1、商品（CD 等）1 9 1 2、店入口 1 9 1 3 等から構成される。店員 1 9 1 1 は、携帯端末 0 2 1 1 として店員カードを所有している。また、ユーザ周辺デバイス 0 2 1 8 としては、店頭に並ぶタグ付き商品（CD 等）を想定している。

【0038】

さらに、この適用例のサービスデバイス 0 2 2 0 としては、未精算の商品（CD 等）持ち出しをチェックする警報機付きタグリーダーを常設した店入口 1 9 1 3 を考える。具体的には、精算時商品（CD 等）に貼付されたタグに精算済み情報を書

き込み、店入口 1 9 1 3 にてそのタグを読みとる。読み取った情報に精算済み情報が含まれておらず、かつ商品 (CD等) を所持している者が店員でない場合警報を鳴らすものである。そこで、本発明における周辺デバイス情報を用いたアクセス制御システムの適用例における概略は以下に示す通りである。『未清算の商品 (CD等) 1 9 1 2 を所持した客 1 9 1 0 が店入口 1 9 1 3 に差し掛かると警報機が鳴るが、店員 1 9 1 1 が商品 (CD等) 1 9 1 2 を所持して店入口を通過しても警報機は鳴らない。』さらに詳述すると、以下のようである。

【 0 0 3 9 】

1. 客 1 9 1 0 が未清算のまま店入口 1 9 1 3 を通過しようとする、商品 (CD等) タグ (未清算情報を含む) が入口付近に常設されたリーダによって読み取られる。
2. 読み取られた情報が、商品の未清算情報である場合、リーダの警報機が作動する。
3. 店員 1 9 1 0 が未清算の商品 (CD等) 1 9 1 2 を所持したまま店入口 1 9 1 3 を通過しようとした場合は、店員 1 9 1 1 の所有する店員カード及び商品 (CD等) タグ (未清算情報を含む) が入口付近に常設されたリーダによって読み取られる。
4. 読み取られた情報が、店員情報である場合商品 (CD等) 1 9 1 2 のタグ情報に書き込まれた精算/未清算情報に依らずリーダの警報機は作動しない。

【 0 0 4 0 】

図 2 1 は、本発明におけるアクセス制御方法を適用した実施例 3 を示す概略図である。主な構成要素として、社員 A 2 1 1 0、社員 B 2 1 1 1、エレベータ 2 1 1 2 等から構成される。社員 A 2 1 1 0 及び社員 B 2 1 1 1 は、携帯端末等を用いてエレベータ 2 1 1 2 を要求する階に呼び出す。社員 A は、エレベータ 2 1 1 2 からある一定の距離 (近傍距離閾値) 2 1 1 3 以上の場所からサービスを要求し、社員 B は、近傍距離閾値 2 1 1 3 を半径とする円内からサービスを要求する。そこで、本発明における周辺デバイス情報を用いたアクセス制御システムの適用例における概略は以下に示す通りである。『エレベータから遠くの場所 (近傍距離閾値 2 1 1 3 以上離れた場所) に居る社員 A 2 1 1 0 はエレベータ 2 1 1

2 を呼び出せないが、近く（近傍距離閾値 2 1 1 3 を半径とする円内領域）に居る社員 B はエレベータ 2 1 1 2 を呼び出すことができる。』さらに詳述すると、以下のようである。

【 0 0 4 1 】

1. 社員 A 2 1 1 0 は、携帯端末等を用いてエレベータ 2 1 1 2 に対してエレベータ呼び出しの要求メッセージを送信する。
2. 携帯端末からメッセージが送信された時間とエレベータ 2 1 1 2 で受信した時間差等を用いて、エレベータと社員 A の携帯端末等との距離を測定する。但し、距離の測定方法に関しては他の方法でもよい。
3. 上記の測定距離が近傍距離閾値 1 2 1 3 以上の場合、エレベータはアクセスを許可しない。
4. 逆に、社員 B 1 2 1 1 のように、測定距離が近傍距離閾値以下の場合、エレベータはアクセスを許可し社員 B 2 1 1 1 に対してサービスを提供する。

【 0 0 4 2 】

図 2 2 は、本発明におけるアクセス制御方法を適用した実施例 4 のシステムの構成図である。主な構成要素は、社員 2 2 1 0、不審者 2 2 1 1、社員所有の携帯端末 2 2 1 2、不審者所有の携帯端末 2 2 1 3、正門 2 2 1 4、履歴情報 DB 2 2 1 5、持出物 2 2 1 6 等から構成される。

【 0 0 4 3 】

そこで、本発明における周辺デバイス情報を用いたアクセス制御システムの適用例における概略は以下に示す通りである。『携帯端末 2 2 1 2 を所持した社員 A は正門を通過できるが、携帯端末 2 2 1 3 を所持しているにも関わらず積極的に個人情報を送信しようとはせず、持出物 2 2 1 6 を持ち出そうとしている不審者 2 2 1 1 が正門を通過しようとするときチェックがかかる。周辺機器構成と併せて、持出物 2 2 1 6 の履歴情報 DB 2 2 1 5 を用いることで、不審者 2 2 1 1 は正門を通過できない。』さらに詳述すると、以下のようである。

【 0 0 4 4 】

1. 携帯端末 2 2 1 2 を所持した社員 A 2 2 1 0 が正門を通過しようとするとき、上記携帯端末 2 2 1 2 から個人情報を獲得する。

2. 社内DB等の参照を行い、上記社員Aが社員であることを確認し正門を通過させる。

3. 携帯端末2213、持出物2216を所持する不審者2211が正門を通過しようとする、携帯端末2213から個人情報が取り出せない。通信は確立されているが、意図的に個人情報等のデータを送信しないようにしている場合等である。

4. 持出物2216の履歴情報DB2215を参照する。

5. 対象機器2611を、持出物2216、参照開始点2612を図書、参照終了点2613を正門、履歴情報2614を不審者2211の行動履歴情報（時刻2510、状態（値）2511、周辺機器2512）としてアクセスレベルを決定する。

6. 周辺機器構成を用いて得られるアクセスレベルと上記アクセスレベルを比較して、ある政策（例えば、アクセスレベルの低い方を優先する等）に従ってアクセスレベルを決定する。

7. 決定されたアクセスレベルに従ってアクセス制御を行う。

【0045】

図25は、本発明におけるユーザ／機器の履歴情報データベースの構成図である。主な構成要素として、時刻2510、状態（値）2511、周辺機器2512等から構成される。時刻2510は、ある対象となるユーザ／機器の履歴情報を採取した時刻（日付情報等含む）である。状態（値）2511は、時刻2510における対象ユーザ／機器の状態値である。例えば、対象が図書の書籍であるような場合は、「貸出未申請」「貸出既申請」等である。周辺機器2512は、時刻2510、状態（値）2511時における対象物ユーザ／機器の周辺に存在する機器である。

【0046】

図26は、本発明における履歴情報データベースを用いた場合のEACLを示す図である。主な構成要素として、アクセスレベル2610、対象機器2611、参照開始点2612、参照終了点2613、履歴情報2614等から構成される。アクセスレベル2610は、本EACLにおいて決定される対象機器2611のアク

セスレベルである。参照開始点 2 6 1 2 は、である。参照終了点 2 6 1 3 は、である。履歴情報 2 6 1 4 は、対象機器 2 6 1 1 の参照開始点 2 6 1 2 から参照終了点 2 6 1 3 間における、ある対象者の行動履歴情報（状態（値） 2 5 1 0、時刻 2 5 1 1、周辺機器 2 5 1 2）ある。

【 0 0 4 7 】

図 2 4 は、本発明におけるアクセス制御方法を適用した実施例 5 のシステム構成図である。主な構成要素は、午前にサービスを要求する社員 A 2 4 1 0、午後にサービスを要求する社員 A 2 4 1 1、部屋のドア 2 4 1 2 等から構成される。そこで、本発明における周辺デバイス情報を用いたアクセス制御システムの適用例における概略は以下に示す通りである。『社員 A 2 4 1 0 及び 2 4 1 1 は、午前中に申請すれば部屋に入ることができるが、午後に申請すると入れない。』さらに詳述すると、以下のようである。

【 0 0 4 8 】

1. 午前中に社員 A 2 4 1 0 が部屋への入室許可申請メッセージを送信する。
2. 上記メッセージは、上記実施例 1 乃至 4 と同様に周辺機器構成、周辺機器状態等を含んでいる。
3. 社員 A 2 4 1 0 が午前中に申請を行った場合、部屋への入室が許可される。
4. 社員 A 2 4 1 1 が午後から申請を行った場合、
上記周辺機器情報等が同一でも、部屋への入室は許可されない。
5. また、社員 A 2 4 1 0 及び 2 4 1 1 が申請を行った時間に関わらず、サービス提供時の時間（帯）（部屋の利用時間等）によって入室許可を発行するという実施例も含む。

【 0 0 4 9 】

図 2 0 は、本発明におけるアクセス制御方法を適用した実施例 6 のシステムの構成図である。主な構成要素として、サービス要求デバイス 2 0 1 0、アクセスレベル認証局 2 0 1 2、サービス配信デバイス 2 0 1 3 等から構成される。サービス要求デバイスは、サービス配信デバイス 2 0 1 3 に対してサービス要求を送信する。この場合、ユーザ 2 0 1 0 及びユーザ周辺デバイス 0 2 1 8 の情報とともにサービス要求を送信する。上記要求を受信したサービス配信デバイス 2 0 1

3は、アクセスレベル照会処理2014を用いてアクセス認証局2012にアクセスレベルの照会を行う。その際、サービス要求デバイス2010から受信した情報及び機器周辺デバイス0228情報を送信する。上記情報を受信したアクセスレベル認証局2012は、EACLを用いてアクセスレベルを決定し、サービス配信デバイス2013に送信する。上記アクセスレベル情報を受信したサービス配信デバイス2013は、受信したアクセスレベルに応じたサービスを提供する。本構成を用いたシステムにおける実施例は、上記実施例1乃至5に該当する。

【0050】

上述した実施例は、以上詳述したように構成されており、次のような効果を奏する。(1) サービス受信側と送信側の周辺状態を含めた木目の細かいアクセス制御が可能となる。(2) ユーザ/サービスデバイスの周辺状態の変更に対して柔軟なアクセス制御が可能となる。

【0051】

【発明の効果】

本発明によれば、アクセス制御などのサービス提供を、きめ細かく実行することが可能になる。

【図面の簡単な説明】

【図1】 本発明におけるアクセス制御システムの適用形態例を示した図である。

【図2】 本発明におけるアクセス制御システムの構成図である。

【図3】 本発明におけるシステム全体の処理を示すフローチャートである。

【図4】 本発明における携帯端末上の周辺デバイス検出処理を示すフローチャートである。

【図5】 本発明における携帯端末上の機器構成管理処理を示すフローチャートである(非常駐処理)。

【図6】 本発明における携帯端末上の機器構成管理処理を示すフローチャートである(常駐処理)。

【図7】 本発明におけるサービスデバイス上の周辺デバイス検出処理を示すフローチャートである。

【図8】 本発明におけるサービスデバイス上の機器構成管理処理を示すフローチャートである。

ャートである（非常駐処理）。

【図 9】本発明におけるサービスデバイス上の機器構成管理処理を示すフローチャートである（常駐処理）。

【図 10】本発明においてユーザが携帯端末を介してサービスを要求する際に送信するメッセージを示した図である。

【図 11】本発明におけるユーザから送信の情報を示す図である。

【図 12】本発明におけるユーザ周辺デバイス情報を示す図である。

【図 13】本発明における周辺デバイス情報を利用したEACLを示す図である。

【図 14】本発明におけるアクセスレベルと実行許可処理との関係を示す図である。

【図 15】本発明における周辺デバイスの判定基準を示す図である。

【図 16】本発明における周辺閾値（近傍距離閾値）の既定方法を示す図である。

【図 17】本発明におけるサービスによる異なる周辺距離の例を示す概略図である。

【図 18】本発明におけるアクセス制御方法を適用した実施例 1 を示す概略図である。

【図 19】本発明におけるアクセス制御方法を適用した実施例 2 を示す概略図である。

【図 20】本発明におけるアクセス制御方法を適用した実施例 6 のシステムの構成図である。

【図 21】本発明におけるアクセス制御方法を適用した実施例 3 のシステム構成図である。

【図 22】本発明におけるアクセス制御方法を適用した実施例 4 のシステム構成図である。

【図 23】本発明におけるサービス要求／提供時の時間（帯）によってアクセスレベルが変化するEACLを示す図である。

【図 24】本発明におけるアクセス制御方法を適用した実施例 5 のシステム構成図である。

【図 2 5】本発明におけるユーザ／機器の履歴情報データベースの構成図である。

【図 2 6】本発明における履歴情報データベースを用いた場合のEACLを示す図である。

【図 2 7】本発明における履歴情報データベースを用いた場合のシステム全体の処理を示すフローチャートである。

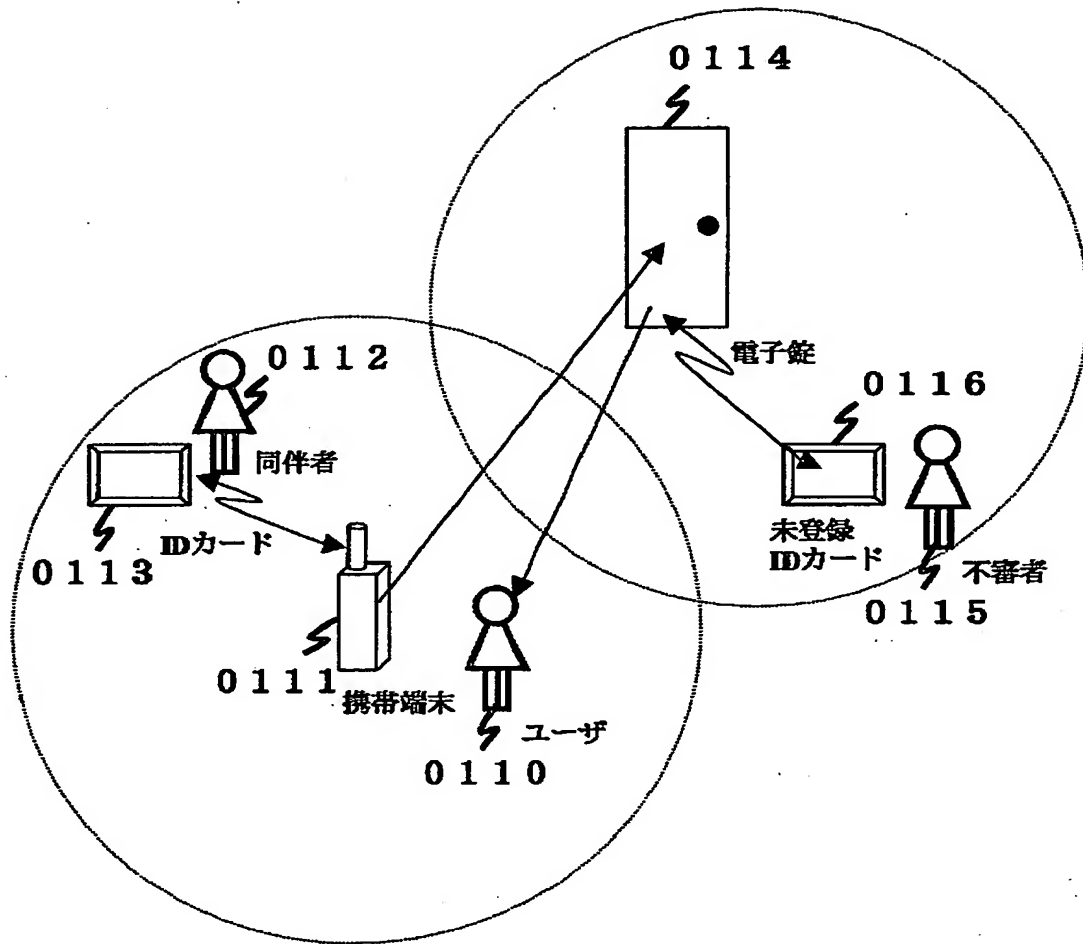
【符号の説明】

0 2 1 0 …システムサービスの対象となるユーザ、0 2 1 1 …携帯端末、0 2 1 2 …携帯端末のI/O、0 2 1 3 …アプリケーションプログラム、0 2 1 4 …データベース、0 2 1 8 …周辺デバイス、0 2 2 0 …サービスデバイス、0 2 2 1 …アプリケーションプログラム、0 2 2 3 …EACLのファイル本体、0 2 2 6 …データベース、0 2 2 8 …周辺デバイス。

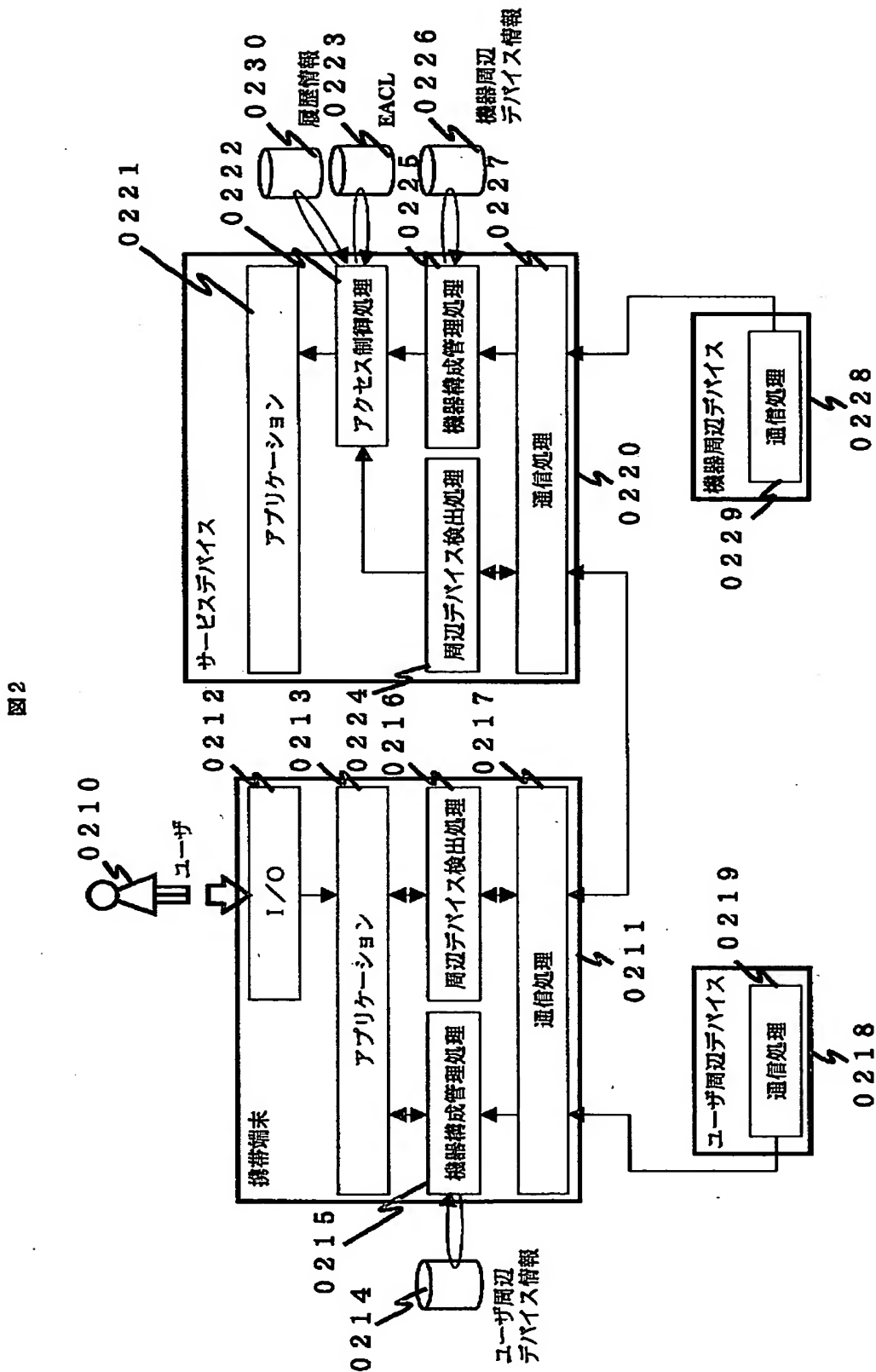
【書類名】 図面

【図1】

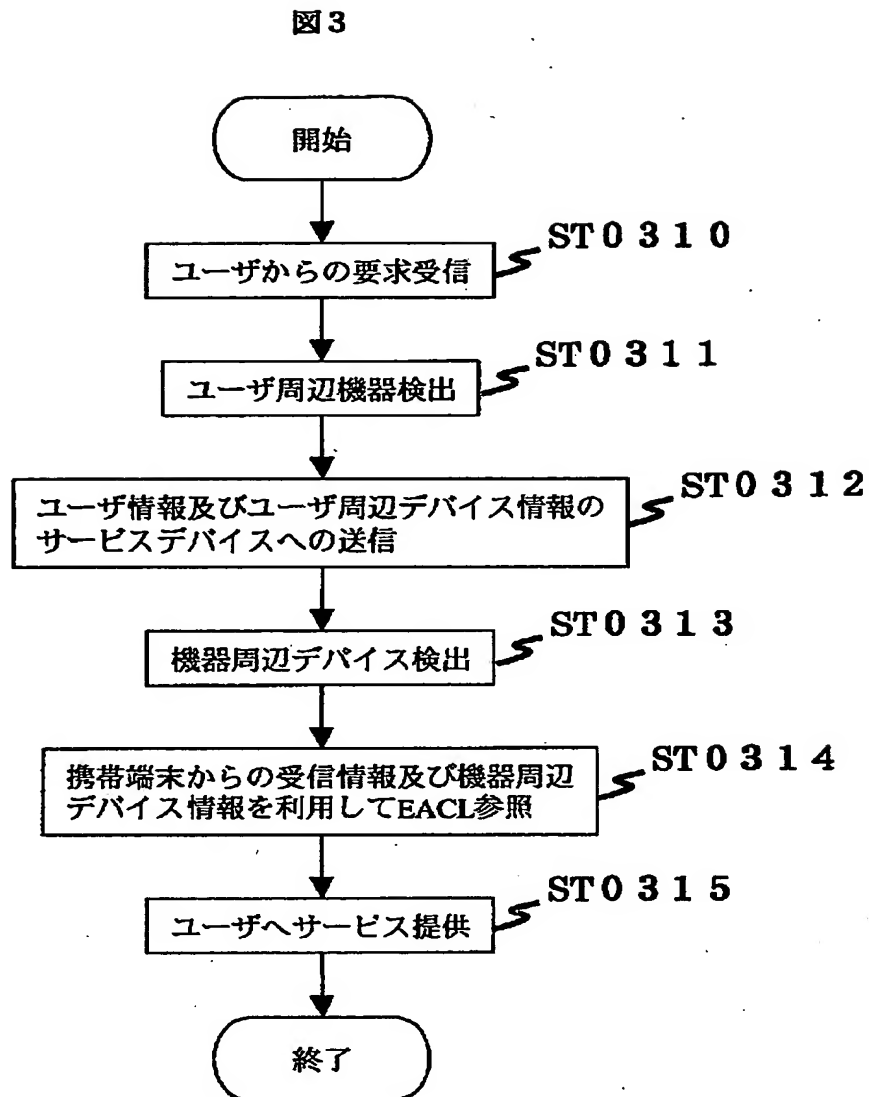
図1



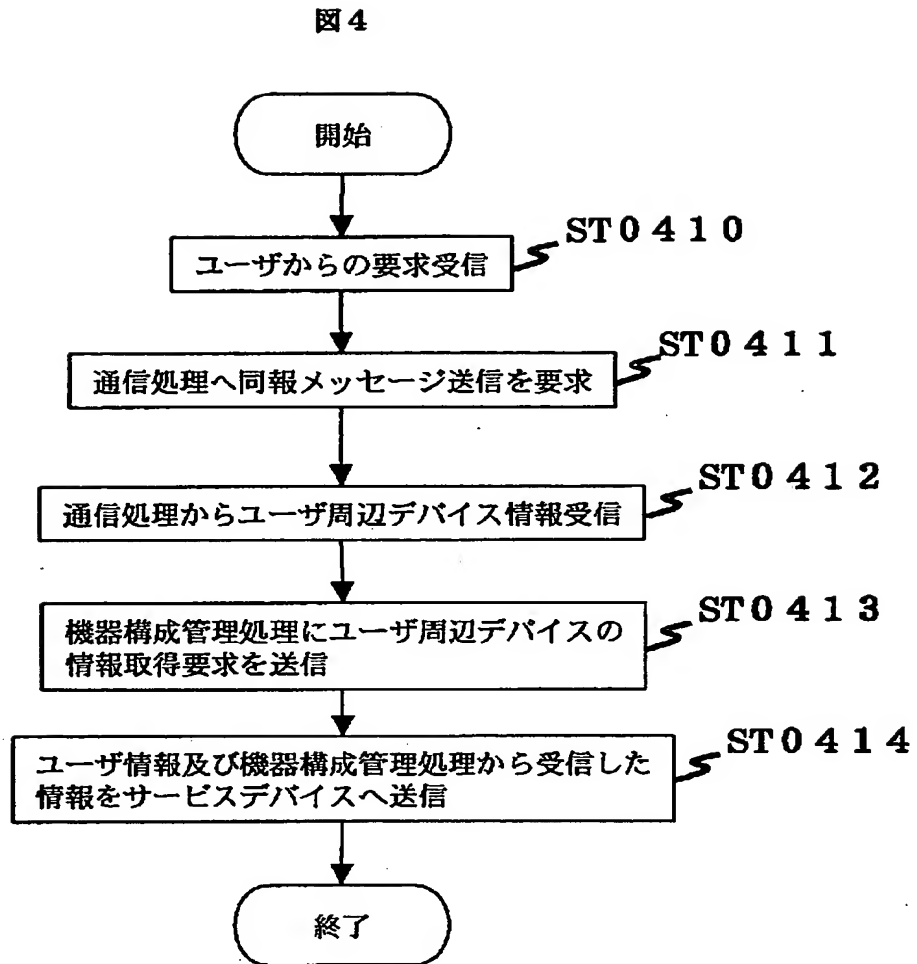
【図 2】



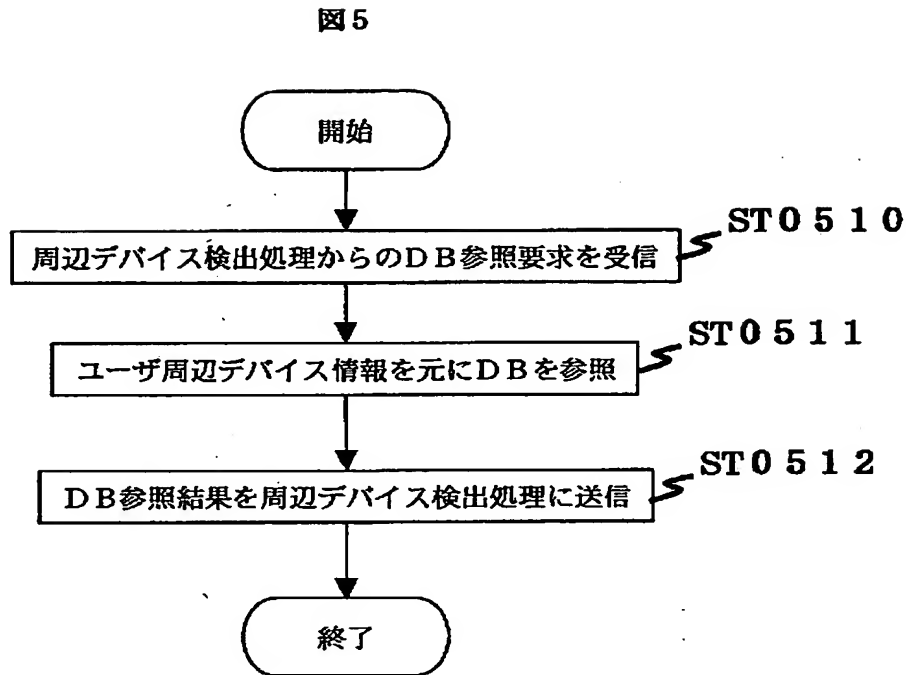
【図3】



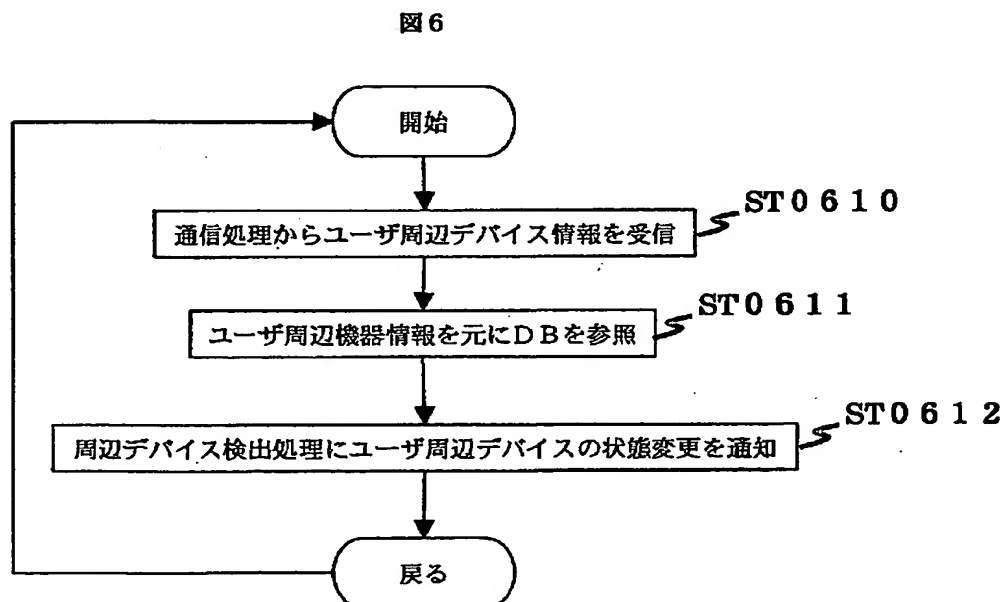
【図 4】



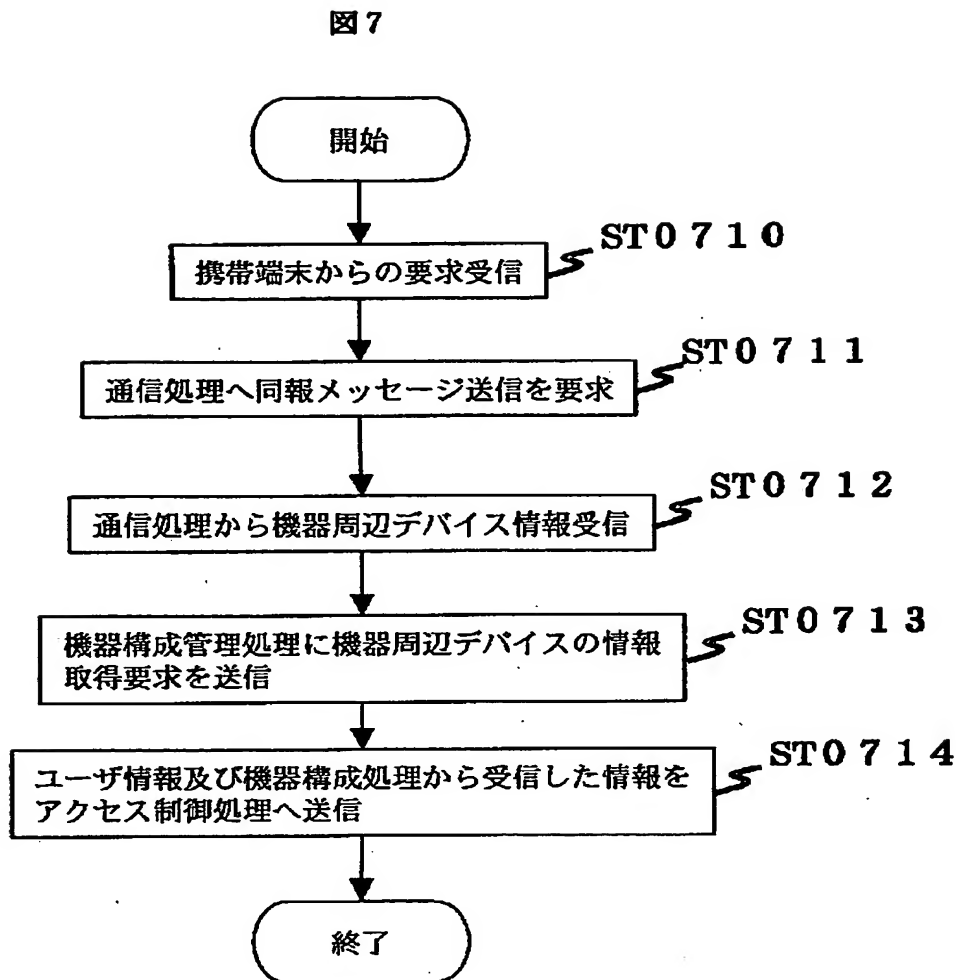
【図 5】



【図 6】

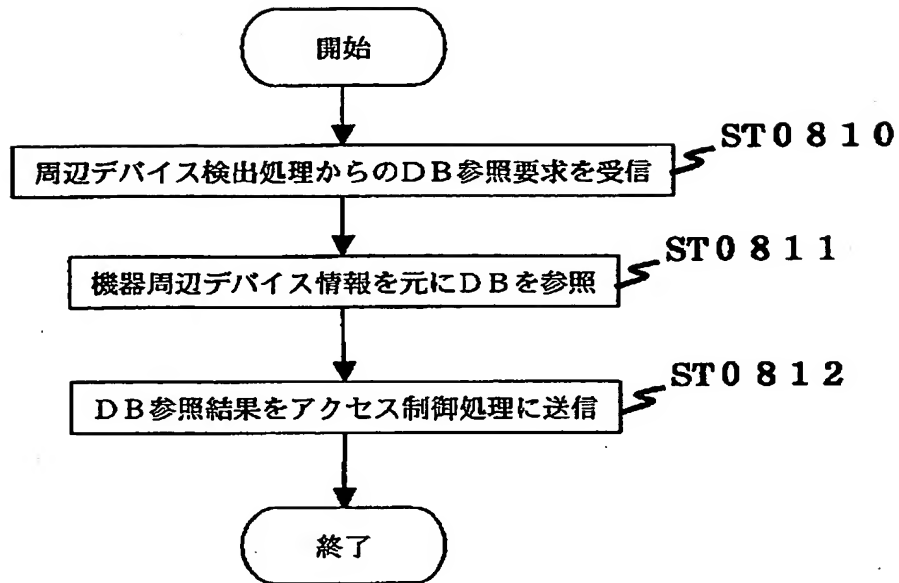


【図 7】



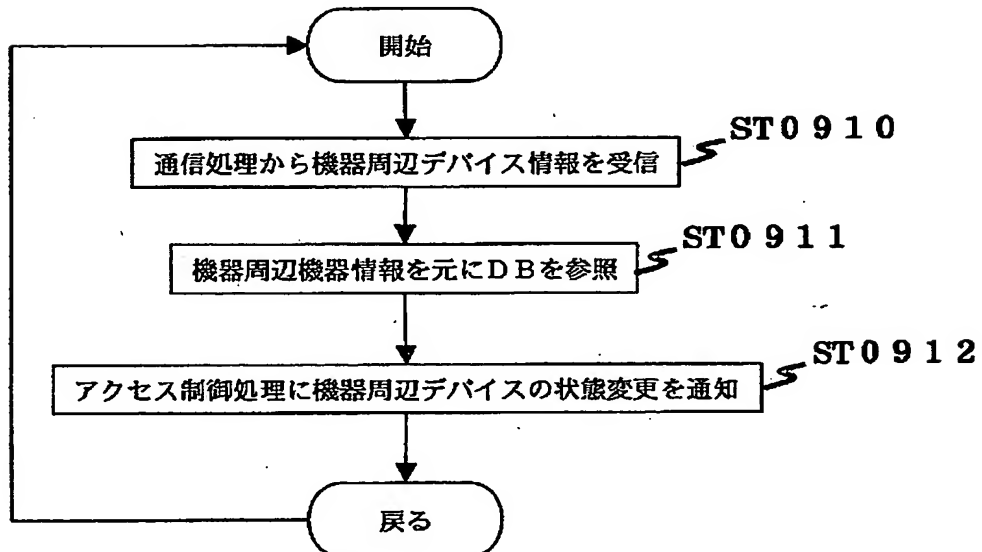
【図 8】

図 8



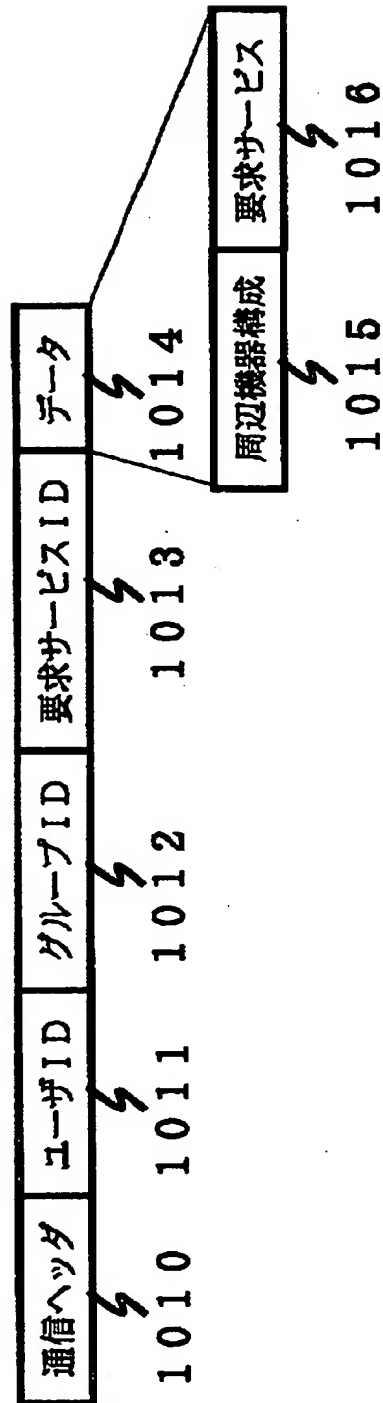
【図 9】

図 9



【図 10】

図 10



【図 11】

図 11

| | 1110 | 1111 | 1112 | 1113 |
|-----|------------------|---------------|---------|--------------|
| # | データ送信日時 | ユーザID | グループID | 要求サービスID |
| 1 | 2001062712235606 | usr_676001027 | grp_105 | e-key_room_a |
| 2 | 2001082015231302 | usr_676001028 | grp_301 | print_room_b |
| ... | ... | ... | ... | ... |

【図 1 2】

図 1 2

| # | データ受信日時 | ユーザ周辺デバイス情報 |
|-----|------------------|-------------|
| 1 | 2001062712235606 | [info_udev] |
| 2 | 2001082015231302 | [info_udev] |
| ... | ... | ... |

【図 13】

図 13

| 1310 | 1311 | 1312 | 1313 |
|---------|---------|-------------|-------------|
| アクセスレベル | グループID | ユーザ周辺デバイス情報 | 機器周辺デバイス情報 |
| 1 | grp_105 | [info_udev] | [info_ddev] |
| 2 | grp_301 | [info_udev] | [info_ddev] |
| ... | ... | ... | ... |

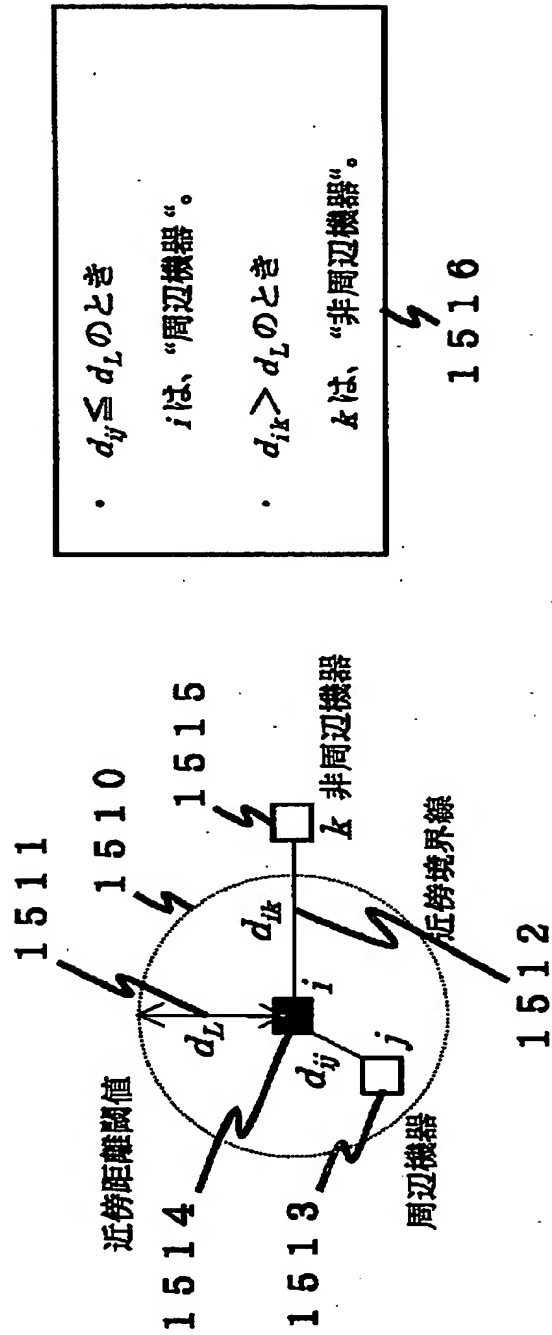
【図 1 4】

図 1 4

| 1 4 1 0 アクセスレベル | 1 4 1 1 実行処理 | 1 4 1 2 アクセス権限 |
|--------------------|-----------------|-------------------|
| 0 | 処理 1 | × |
| | 処理 2 | × |
| | 処理 3 | × |
| | ... | ... |
| 1 | 処理 1 | × |
| | 処理 2 | ○ |
| | 処理 3 | × |
| | ... | ... |
| ... | ... | ... |

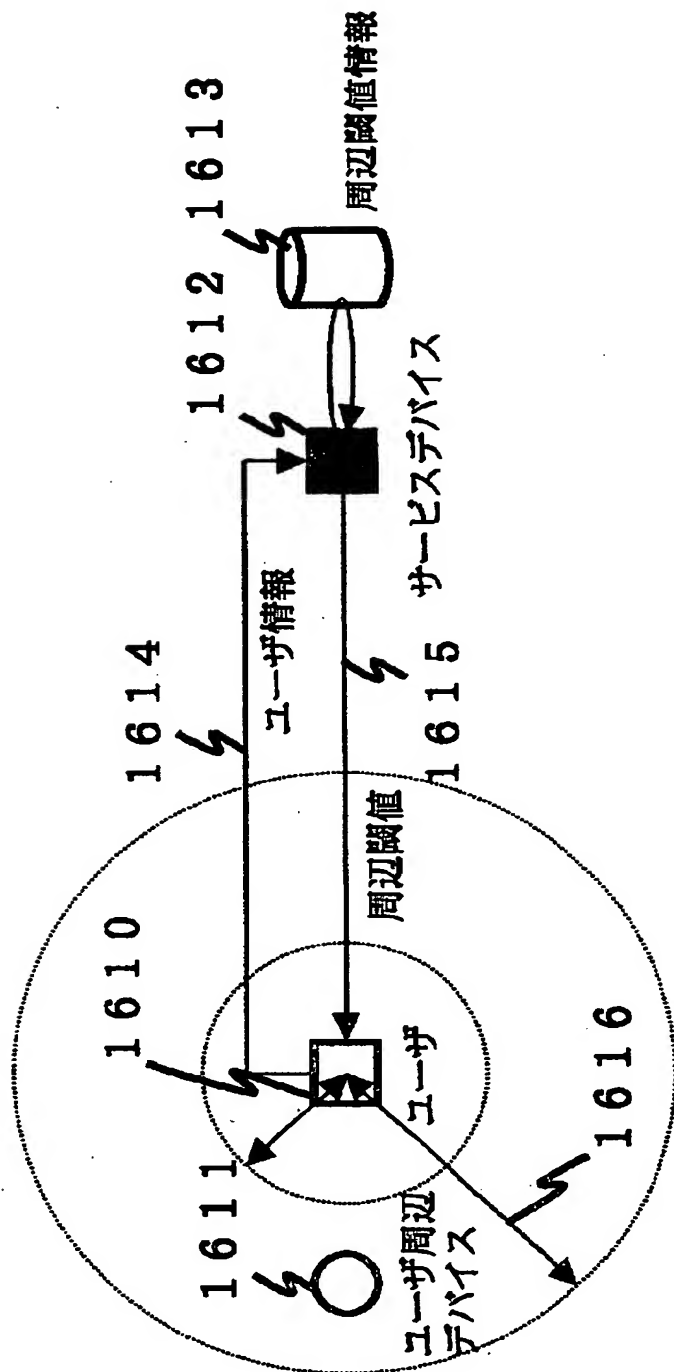
【図 15】

図 15



【図 16】

図 16



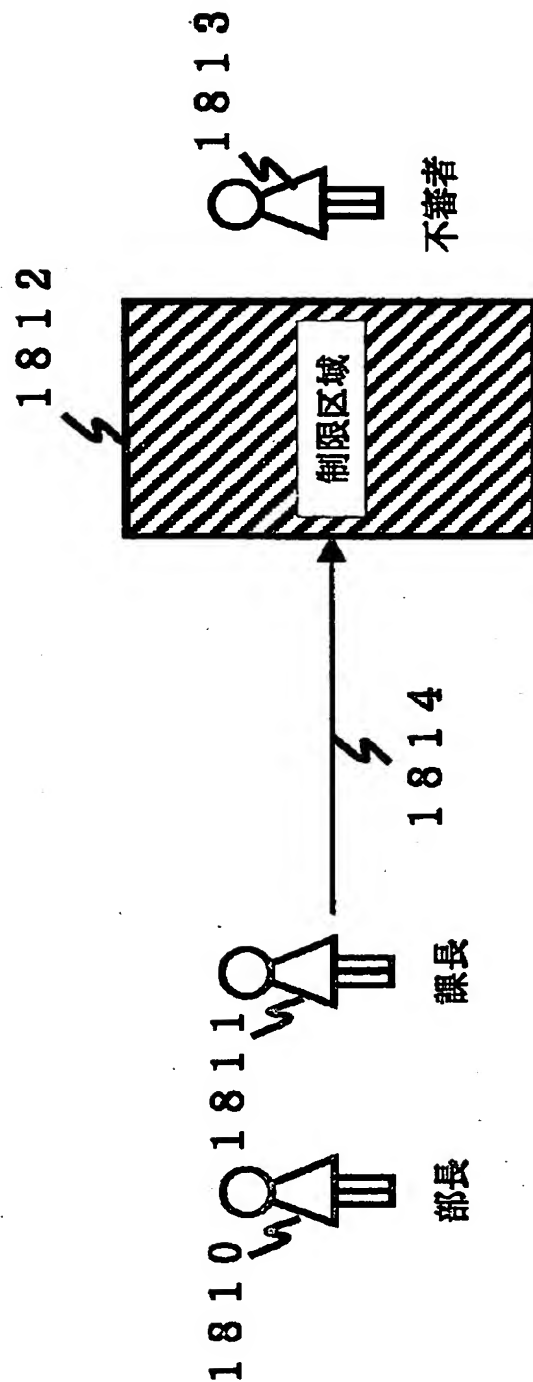
【図 1 7】

図 1 7

| # | サービス | 周辺距離[m] |
|-----|-------|---------|
| 1 | ドアの開錠 | 1 0 |
| 2 | ドアの施錠 | 0 |
| ... | ... | ... |

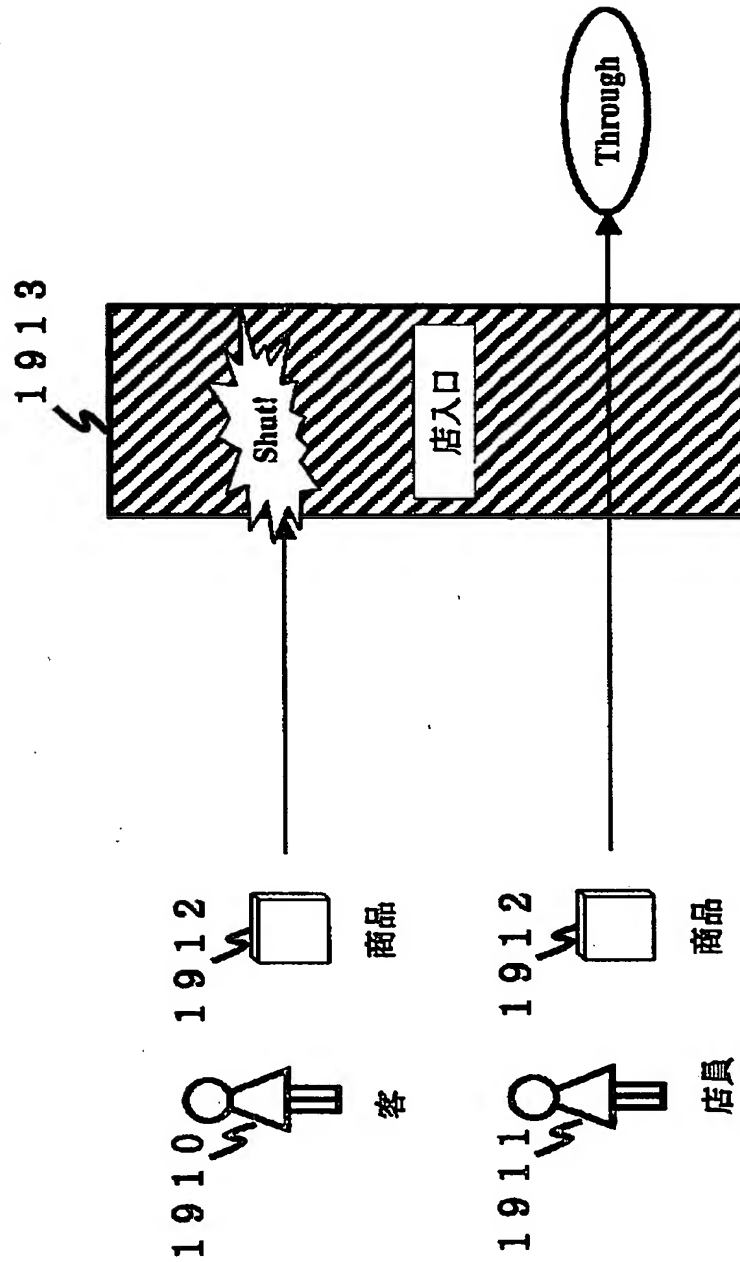
【図 18】

図 18

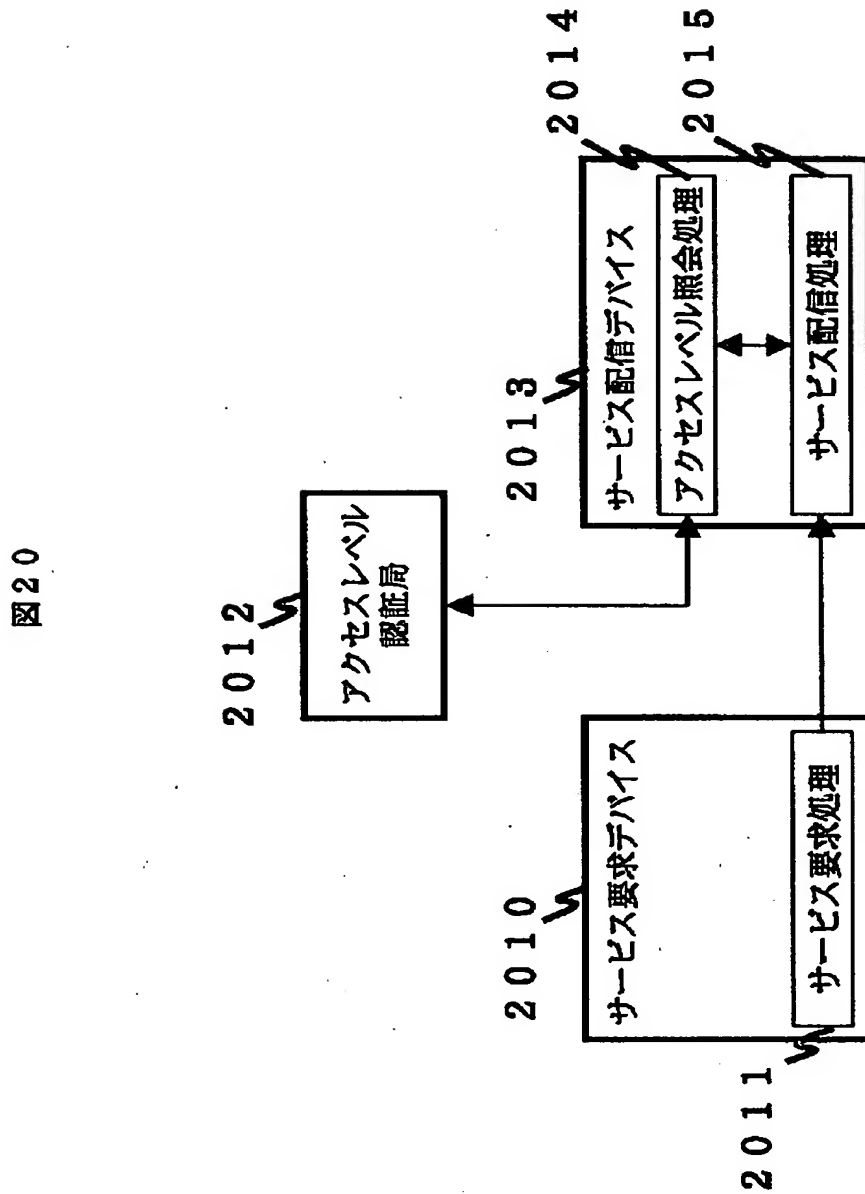


【図 19】

図 19

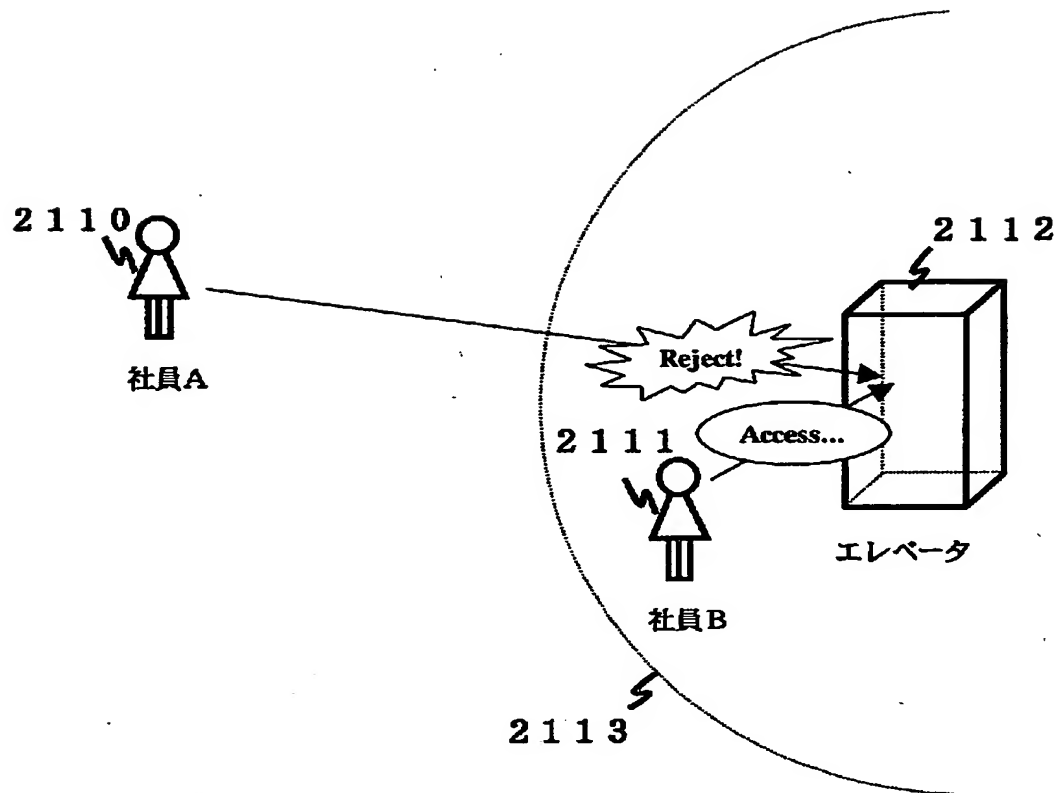


【図20】



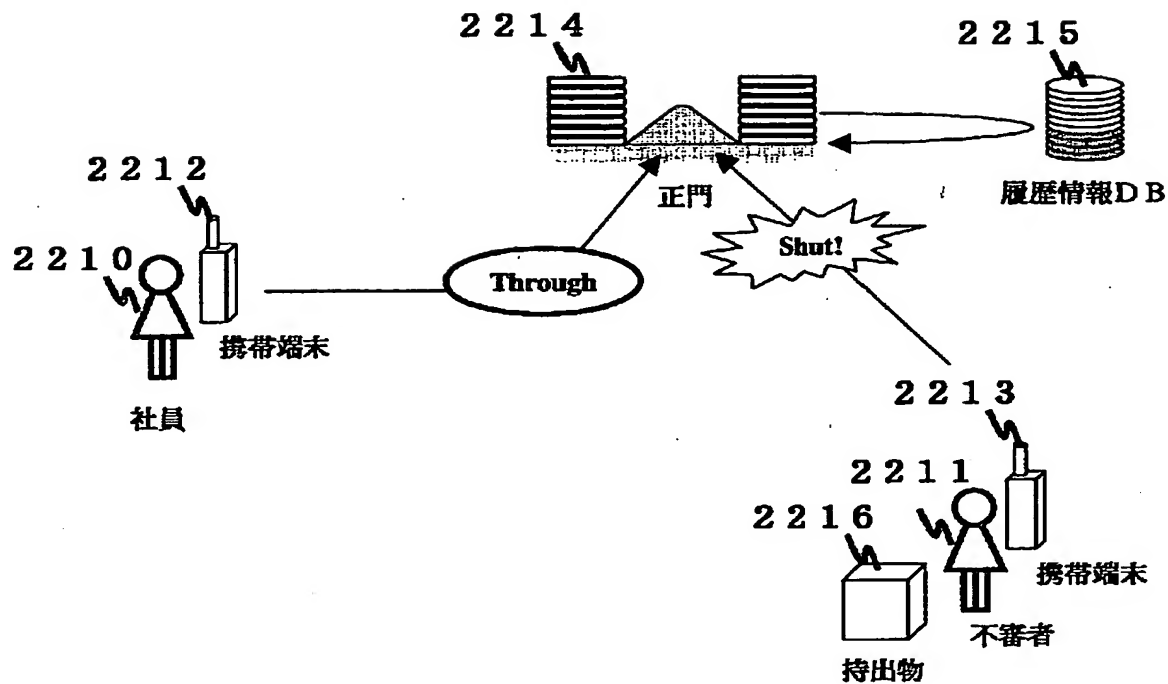
【図 21】

図 21



【図 22】

図 22



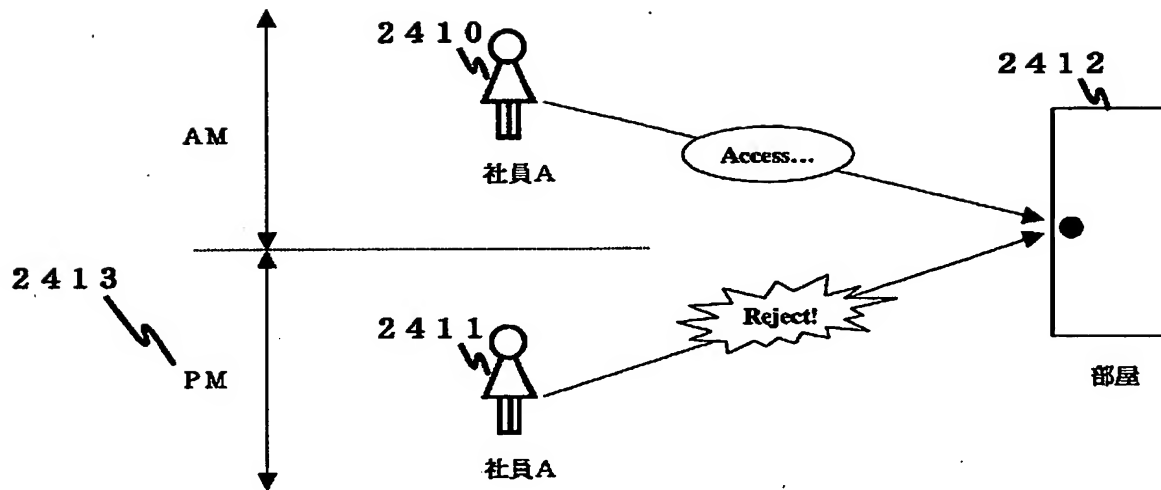
【図 23】

図 23

| 2310 受信情報 | 2311 時間 (帯) | 2312 アクセスレベル |
|--------------|----------------|-----------------|
| inf_receive | AM | 1 |
| inf_receive | PM | 2 |
| ... | ... | ... |

【図 2 4】

図 2 4



【図 2 5】

図 2 5

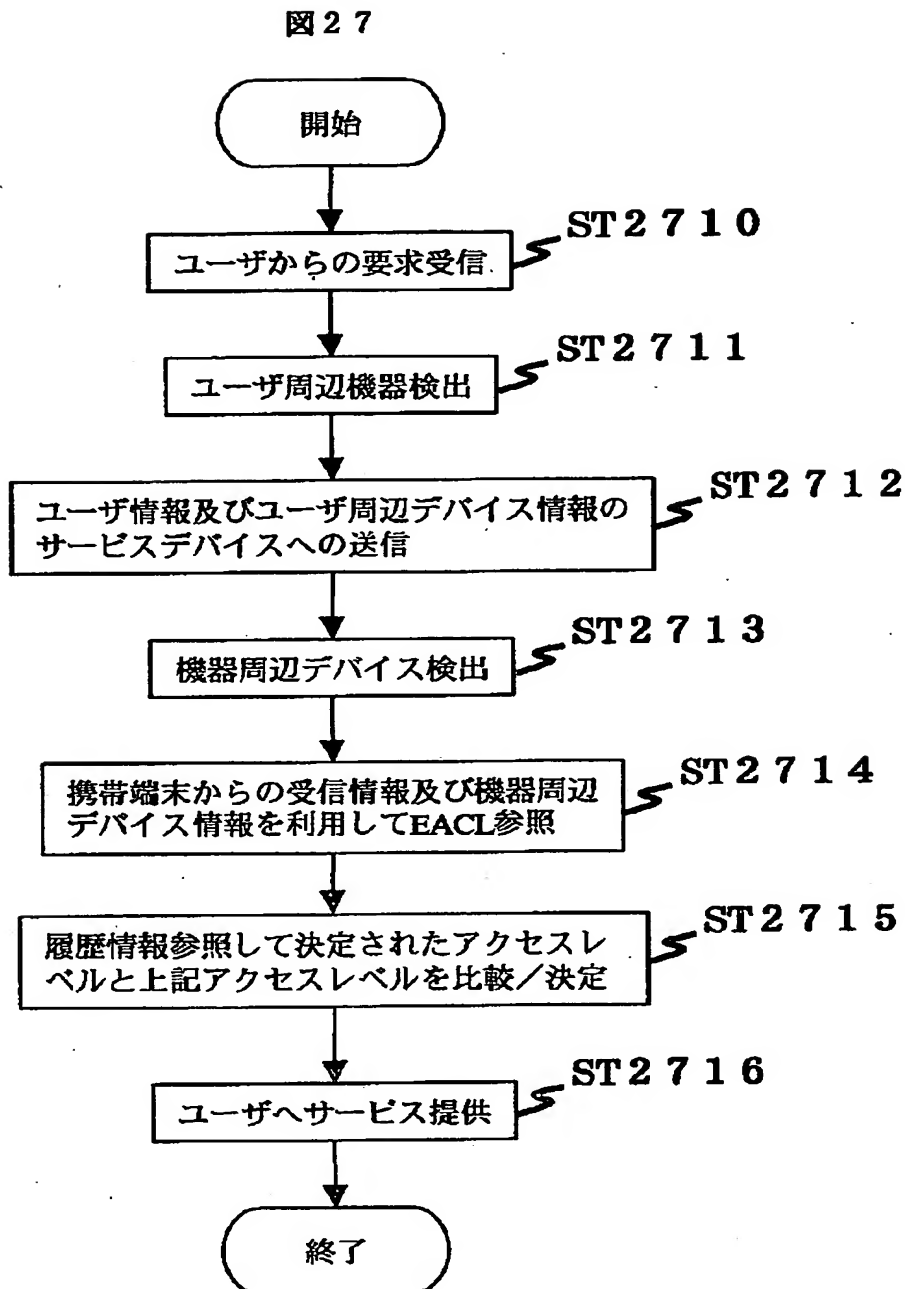
| # | 時刻 (2510) | 状態 (値) (2511) | 周辺機器 (2512) |
|-----|-------------------|---------------|--------------------|
| 1 | 2001.1.1.16:25:06 | ON | PC_2L, ELV_2L, ... |
| 2 | 2001.1.2.12:55:26 | OFF | PC_1L, ELV_1L, ... |
| ... | ... | ... | ... |

【図26】

図26

| 2610 | 2611 | 2612 | 2613 | 2614 |
|---------|------|----------------------|----------------------|-------------------------|
| アクセスレベル | 対象機器 | 参照開始点 | 参照終了点 | 履歴情報 |
| 0 | 機器1 | P: 図書 | P: 正門 | P [要求機器] |
| | | S: 貸出許可 | S: 貸出不可 | P [要求機器], S [要求機器], ... |
| | | T: 2001.1.1.16:25:06 | T: 2001.1.1.16:25:06 | P [要求機器], T [要求機器], ... |
| | | ... | ... | ... |
| | 機器2 | | | |
| 1 | ... | | | |
| | ... | | | |

【図 27】



【書類名】 要約書

【要約】

【課題】

従来においては、様々なユーザが訪問するオフィスビル等において、制限区域内に重要物が存在する場合には入室を禁止し、そうでない場合は許可するような場面を想定した時、従来の画一的なアクセス制御では運用/管理者のアクセスレベルの設定変更作業やユーザの設定変更要求からの時間的な遅れという点で限界があった。

【解決手段】

(1) ユーザ（デバイスにアクセスする人）及びサービスデバイス（ユーザにアクセスされるデバイス）の周辺機器情報を収集する手段を有する。(2) サービスデバイスへのアクセスを許可するか、しないかを判断する手段を有する。

【選択図】 図2

特 2 0 0 1 - 1 7 4 9 8 1

認定・付加情報

| | |
|---------|--------------------------|
| 特許出願の番号 | 特願 2 0 0 1 - 1 7 4 9 8 1 |
| 受付番号 | 5 0 1 0 0 8 3 4 3 2 3 |
| 書類名 | 特許願 |
| 担当官 | 第七担当上席 0 0 9 6 |
| 作成日 | 平成 1 3 年 6 月 1 2 日 |

< 認定情報・付加情報 >

| | |
|-------|-------------|
| 【提出日】 | 平成13年 6月11日 |
|-------|-------------|

次頁無

出 願 人 履 歴 情 報

識別番号 [000005108]

| | |
|----------|--------------------|
| 1. 変更年月日 | 1990年 8月31日 |
| [変更理由] | 新規登録 |
| 住 所 | 東京都千代田区神田駿河台4丁目6番地 |
| 氏 名 | 株式会社日立製作所 |